# Vulnerability Analysis of the Simple Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks

Thomas Heide Clausen, Ulrich Herberg, Jiazi Yi

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# *Vulnerability Analysis of the Simple Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks*

Thomas Clausen, Ulrich Herberg, Jiazi Yi

**N° 7638**

June 2011


ISSN 0249-6399 ISRN INRIA/RR--7638--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
SACLAY - ÎLE-DE-FRANCE

# Vulnerability Analysis of the Simple Multicast Forwarding (SMF) Protocol for Mobile Ad Hoc Networks

Thomas Clausen*, Ulrich Herberg†, Jiazi Yi‡

Thème : COM – Systèmes communicants
Équipe-Projet Hipercom

Rapport de recherche n° 7638 — June 2011 — 21 pages

**Abstract:** If deployments of Mobile Ad Hoc Networks (MANETs) are to become common outside of purely experimental settings, protocols operating such MANETs must be able to preserve network integrity, even when faced with careless or malicious participants. A first step towards protecting a MANET is to analyze the vulnerabilities of the routing protocol(s), managing the connectivity. Understanding how these routing protocols can be exploited by those with ill intent, countermeasures can be developed, readying MANETs for wider deployment and use.

One routing protocol for MANETs, developed by the Internet Engineering Task Force (IETF) as a multicast routing protocol for efficient data dissemination, is denoted "Simplified Multicast Forwarding" (SMF). This protocol is analyzed, and its vulnerabilities described, in this memorandum.

SMF consists of two independent components: (i) duplicate packet detection and (ii) relay set selection, each of which presents its own set of vulnerabilities that an attacker may exploit to compromise network integrity. This memorandum explores vulnerabilities in each of these, with the aim of identifying attack vectors and thus enabling development of countermeasures.

**Key-words:** MANET, multicast, security, vulnerability, SMF, attacks, IETF

* LIX - Ecole Polytechnique - Thomas@ThomasClausen.org
† LIX - Ecole Polytechnique - Urich@Herberg.name
‡ LIX - Ecole Polytechnique - yi.jiazi@gmail.com

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université
4, rue Jacques Monod, 91893 ORSAY Cedex
Téléphone : +33 1 72 92 59 00

# Analyse de Vulnérabilité du Protocole "Simple Multicast Forwarding (SMF)" pour des Réseaux Ad Hoc

**Résumé :** Afin d'augmenter le nombre de déploiements de réseaux ad hoc dehors des "testbeds" purement expérimentals, des protocoles de routage des réseaux ad hoc doivent être en mesure de préserver l'intégrité du réseau, même lorsqu'ils sont confrontés avec des participants imprudents ou malicieux. Un premier pas vers la protection d'un réseau ad hoc est d'analyser les vulnérabilités du protocole de routage qui gère la connectivité du réseau. En comprenant comment ces protocoles de routage peuvent être exploités par des personnes ayant de mauvaises intentions, des contre-mesures peuvent être dveloppées.

Un protocole de routage pour des réseaux ad hoc, développé par l'Internet Engineering Task Force (IETF) comme protocole de routage de multicast pour la diffusion efficace des données, est appelé "Simplified Multicast Forwarding" (SMF). Ce protocole est analysé, et ses vulnérabilités décrites dans ce rapport.

SMF est constitué de deux composantes indépendantes: (i) la détection des paquets dupliqués et (ii) la sélection des relais, dont chacun présente son propre ensemble de vulnérabilités qu'un attaquant peut exploiter pour compromettre l'intégrité du réseau. Ce rapport explore des vulnérabilités dans chacune des deux composantes, afin d'identifier les vecteurs d'attaque, ainsi de permettre de développer des contre-mesures.

**Mots-clés :** MANET, multicast, securité, vulnérabilité, SMF, attaques, IETF

# 1 Introduction

Network integrity in wired, multi-hop networks is largely preserved by physically controlling access to the communications channel between routers: know thy peers, know which behavior to expect from thy peers, trust thy peers – and be able to disconnect thy peers if they show not worthy of that trust. In a MANET (Mobile Ad hoc NETwork), often operated over wireless interfaces, such is less obvious: physical access to the media between routers is not delimited by a cable, but is available to anyone within transmission range; the network topology is time-varying, either due to router mobility or due to time-varying characteristics of the channel; traffic is often retransmitted over the same wireless interface as the one over which it was received. Consequently, MANET protocols are conceived to manage conditions where less – or no – a-priori structure is present between peers, and are exposed to characteristics not commonly found in classic wired networks.

This exposure also renders MANET protocol more vulnerable to attacks, although two things shall be noted. First, MANET protocols by way of their lack of a-priori infrastructure knowledge and lack of physical access control to the communications channel are simply "exposing" and rendering more easily exploitable vulnerabilities already present in classic networks (*e.g.,* such as injecting rouge traffic in a network). Second, MANET protocols having to manage specific characteristics (*e.g.,* retransmission of traffic on an interface over which it was received), introduces new, specific protocol mechanisms, which may be open to attacks.

## 1.1 Background and History

The "Simple Multicast Forwarding" (SMF) protocol [1] is a multicast routing protocol for MANET-wide efficient broadcasting, employing reduced relay sets for decreasing the number of redundant retransmissions of a data packet. Reduced relay sets so used were introduced in and standardized for IP networks by way of the Optimized Link State Routing Protocol (OLSR [2]) in 2003, where such were used for substantially reducing the protocol overhead incurred by diffusion of routing protocol control traffic (link state advertisements, in [2] denoted "TC messages"). The reduced relay set mechanism in OLSR is based on Multi-Point Relays (MPRs) [3]. This concept was retained and used in an extension of OSPF for MANET areas [4]. The reactive MANET routing protocol AODV [5] also uses MANET-wide broadcast of its control traffic (route requests). [6] showed that using MPRs for flooding such control traffic resulted not just in reduced channel load, but also in shorter unicast paths. Other experimental routing protocols, including [7] and [8], have used different relay set selection mechanisms, and the Internet Engineering Task Force (IETF) is standardizing the MANET routing protocol OLSRv2 [9], retaining the MPR concept.

The success of such reduced relay sets for protocol control traffic diffusion lead to investigations into using such also for user data traffic, including [10] and [11], ultimately leading to the IETF proposing development of SMF [1] as an experimental protocol.

## 1.2 SMF Overview

SMF provides basic IP multicast routing for MANETs. It consists of two main components: multicast "Duplicate Packet Detection" (DPD) and "Relay Set Selection" (RSS).

### 1.2.1 Multicast Duplicate Packet Detection (DPD)

DPD is used as part of the forwarding process to check if an incoming packet has been previously received (and forwarded) – and therefore should be dropped – or not. In MANETs, as illustrated in figure 1, duplicate packets are a common fact of life: router `n1` is retransmitting a broadcast packet received from router `n0` on the same interface as the one over which it was received, so as to ensure receipt also by router `n2` – causing router `n0` to receive the packet a second time.

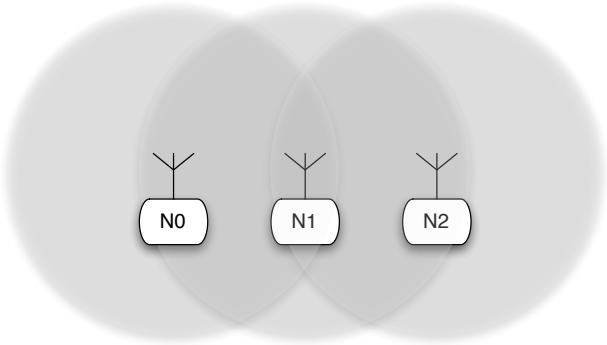


Figure 1: The need for duplicate detection: retransmission over the same interface as a packet was received.

DPD is achieved by a router maintaining a record of recently processed multicast packets, and comparing received multicast packets herewith. A duplicate packet detected is silently dropped and not inserted into the forwarding path of that router, nor delivered to an application. DPD, as proposed by SMF, supports both IPv4 and IPv6 and for each suggests two duplicate packet detection mechanisms: 1) header content identification-based DPD (I-DPD), using packet headers, in combination with flow state, to estimate temporal uniqueness of a packet, and 2) hash-based DPD (H-DPD), employing hashing of selected header fields and payload for the same effect.

### 1.2.2 Relay Set Seletion

RSS produces a reduced relay set for use when relaying information across the MANET. SMF supports the use of several relay set algorithms, including E-CDS (Essential Connected Dominating Set), S-MPR (Source-based Multi-Point Relay), or MPR-CDS. Those algorithms are based on localized election, derived from those explored for efficient topology diffusion in MANET routing protocols.

### 1.3 Statement of Purpose

While multicast protocols and efficient flooding mechanisms are well studied for performance and convergence properties, little work considers also security issues and implications of the protocols in use – which assume that the routers in the networks can be "trusted" to perform properly. In any deployment scenario, however, this assumption cannot be taken at face value: the "accessibility" of a wireless communications channel may open access to malicious routers attempting to participate in the network – or an otherwise non-malicious router may simply be misconfigured.

If deployments of MANETs are to become common outside experimental settings, protocols operating in such networks must be resilient to such malice or misconfiguration. A first step towards such resilience is to understand the vulnerabilities of a given protocol and identify probable attack vectors hereon.

This memorandum analyses SMF in order to understand its vulnerabilities. Various threats, from accidental misbehavior of routers or from intentionally malicious attackers, are studied, and threat sources, threat actions, threat consequences, etc. are explored. While the study is generally based on SMF, the components of SMF, such as duplicate packet detection and relay set selection, are common in other multicast routing protocols, and may therefore be also more generally applicable.

While the memorandum has the ambition of being thorough, in matters of security it is prudent to be explicit to not claim completeness of an analysis.

### 1.4 Memorandum Outline

The remainder of the memorandum is organized as follows. In section 2, threats to DPD are first discussed. Possible attacks to the *Relay Set Selection Vector* (RSSV), which is used for identify different types of RSS algorithms, are presented in section 3. The general threats to RSS are presented in section 4. The memorandum is concluded in section 5.

## 2 Threats to Duplicate Packet Detection

The DPD mechanism is based on a unique identity check of the incoming packets. A router needs to record a history of processed multicast packets so as to ensure that a given packet is processed and forwarded at most once – which entails that such history must be maintained for at least the maximum network traversal time of a packet. However, neither IPv4 nor IPv6 contains mechanisms for uniquely identifying a given packet. SMF introduces two mechanisms compensating this: I-DPD and H-DPD. This section discusses attacks on each of these, as well as the consequences on protocol operation that such may have.

### 2.1 Identification-based DPD (I-DPD)

For I-DPD, a DPD identifier in the packet header is used for identification of a packet. In case of fragmented packets, and packets using IPsec, the contained fragment and packet sequence numbers can be used. When neither is present, an additional identifier in the packet header is needed. SMF proposes an IPv6

header option to this effect, recognizing that adding such IP packet header information is not supported for IPv4.

The identification of a packet is, then, based on the source IP address and the sequence number (from IPsec, fragment number or header option). In this way, when each intermediate router receives a packet, it can determine if the packet has been received before.

### 2.1.1 Pre-play Attack

If a malicious router can obtain the (source IP, sequence number) of a packet, it can inject (invalid) packets with exactly the same identification information into the network. As such an invalid packets propagates through the network, if arriving before the valid packet with same identification information, this valid packets will be discarded as a duplicate. If further sequence numbers are predictable, a malicious router can inject invalid packets with valid sequence numbers in advance, ensuring that subsequent valid packets are discarded as duplicates.

Figure 2 illustrates an example of a pre-play attack. Router $a$ is the source and generates a multicast packet with sequence number $n$. When the malicious router $X$ receives the packet, it injects an invalid packet with the same sequence number $n$. Routers which receive the invalid packet first will discard subsequent arrivals of the valid packet. The consequence hereof depends on the network topology: as depicted in figure 2, the attack might not affect routers that are farther away from the malicious router than they are from the source router (*i.e.,* routers $e$ and $h$), as the valid packet might reach those routers first. For routers closer to the attacker than to the source (*i.e.,* router $g$ and $f$), the invalid packet will be received first, causing subsequently arriving valid packets to be dropped. For routers with equal distance (router $c$ and $d$), it depends on the link status and the transmission of the routers.

When the succession of sequence numbers from a source is predictable, a malicious router can, upon having observed a valid packet being generated by a legitimate router, conduct a pre-play attack by injecting invalid packets with not-yet-used-but-soon-to-be-used sequence numbers. As shown in figure 3, if an incremental algorithm is used for generating sequence numbers, $X$ can thereby prohibit corresponding valid packets from attaining the part of the network reachable from $X$ without passing through $a$. The following packets from $a$ with $seq = n + 1$, $seq = n + 2$, etc, will be regarded as duplicate packets and discarded.

Another possible pre-play attack is based on the Time-to-Live (TTL) or hop limit field[1]. As routers only forward packets with $TTL > 1$, a malicious router can forward an otherwise valid packet, while drastically reducing the TTL hereof. This will inhibit recipient routers from later forwarding the same multicast packet, even if received with a different TTL – essentially a malicious router thus can instruct its neighbors to block forwarding of valid multicast packets. As the TTL of a packet is intended to be manipulated by intermediaries forwarding it, classic methods such as signatures are typically calculated with setting TTL fields to some pre-determined value (*e.g.,* 0) – such is for example the case for IPsec Authentication Headers'[12] – rendering such an attack

[1]Henceforth, TTL is used indiscriminately for both TTL and hop-limit.

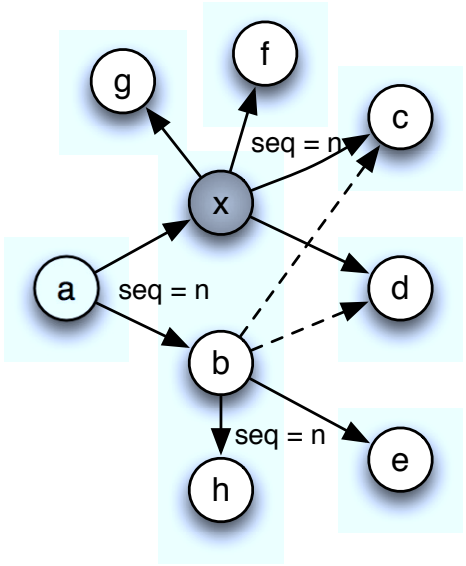


Figure 2: Pre-play attack: `X` is a malicious router, which generates invalid packets with valid sequence numbers.

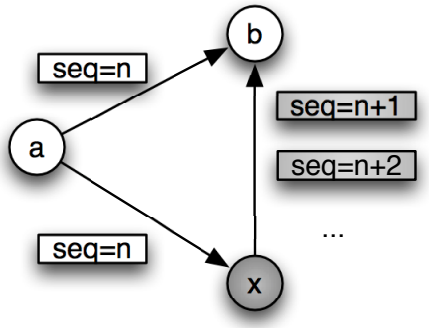


Figure 3: Pre-play attack by predicting sequence number. `X` is a malicious router, which generates invalid packets with predicted sequence number.

more difficult to both detect and counter. If the malicious router has access to a "wormhole" through the network (a directional antenna, a tunnel to a collaborator or a wired connection, allowing it to bridge parts of a network otherwise distant) it can make sure that the packets with such an artificially reduced TTL arrive before their unmodified counterparts.

Figure 4 illustrates an example of this attack, with $X$ being the malicious router. On receiving a packet with $TTL = 63$ and $seq = n$, $X$ broadcasts the same packet, but with an artificially reduced $TTL = 1$. For routers near $X$, such as $c$, $d$, and $e$, if they receive the packet with the artificially reduced TTL before the valid packet arrives, the valid packet will be discarded. If a wormhole between $X$ and a distant router $i$ exists, $X$ can inject the packet

with the artificially reduced TTL to $i$, and to the part of the network reachable through $i$ – which would subsequently discard later arriving valid packets.

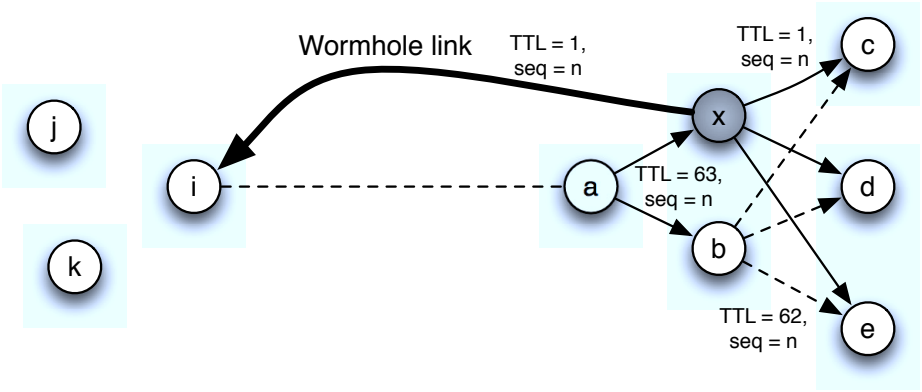


Figure 4: Pre-play attack based on TTL values. $X$ is the malicious router which forwards the packets with reduced TTL values.

### 2.1.2 Sequence Number Attack

In a pre-play attack, a malicious router makes use of the DPD mechanism to force other routers to discard otherwise valid packets – thus preventing these from reach parts of the network. A malicious router can also seek to disable DPD, by modifying the sequence number in packets that it forwards. Thus, routers will not be able to detect an actual duplicate packet as a duplicate – rather, they will treat them as new packets, *i.e.,* process and forward them. The consequence of this attack is an increased channel load, the origin of which appears to be a router other than the malicious router.

In figure 5, when the malicious router $X$ receives the packet (seq = $n$) from router $a$, it simply modifies the sequence number to $n + i$, and sends it back to the network. Router $c$ will not be able to detect the duplicate packet, which should be discarded.

[1] proposes use of IPsec sequence numbers as packet identifiers. If IPsec is used, authentication and integrity of the packets is usually assumed protected. In a MANET environment, the usage of IPsec is still not well defined – problems include key distribution mechanisms, suitable cryptographic algorithms and the use of IPsec for multicast. Furthermore, to the best of the authors knowledge, few deployments of MANETs employ IPsec. Therefore, this memorandum does not consider the usage of the IPsec options as presented in [1].

## 2.2 Hash-based DPD (H-DPD)

In H-DPD, a hash of the non-mutable header fields, options fields and data payload is used as identifier of a packet, replacing explicit sequence numbers. Each packet is, thus, uniquely identified by the IP address of the source of the packet, and this hash-value. When a source host generates a packet, or when a gateway ingresses the packet into the MANET, it calculates the hash-value hereof. In case the source host or gateway identifies that it recently has

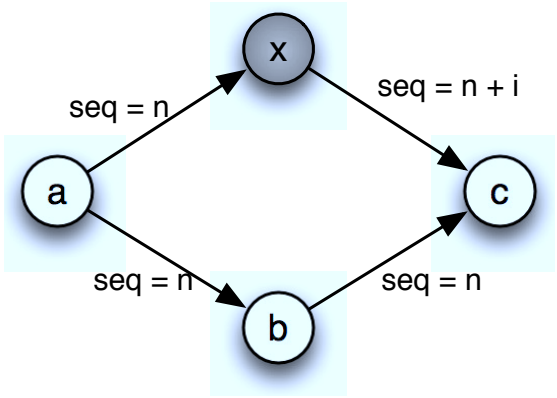


Figure 5: Sequence number attack. $X$ is the malicious router and modifies the sequence number to disturb duplicate packet detection

generated or injected a packet with the same hash-value, it inserts a "Hash-Assist Value (HAV)" IPv6 header option into the packet, shown in figure 6, generated such that calculating the hash also over this HAV will render the resulting value unique.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                ...              |0|0|0| OptType | Opt. Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|    Hash Assist Value (HAV) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: The Hash Assist Value header option in H-DPD mode

Note that the hash value in SMF is applied only to provide a low probability of collision, and is specifically not used for cryptographic or authentication purposes. Also note that threats, similar to those discussed in section 2.1 continue to apply for when using H-DPD. One advantage of H-DPD over I-DPD may be, however, that as the hash-value is calculated also over the data payload of the packets, predicting subsequent hash-values and conducting a pre-play attack is somewhat harder.

Introducing a header option, however, also introduces a potential vulnerability: the HAV header option is only used when the source or the ingressing router detects that a previously generated packet has an identical hash value as this packet. A malicious router which discovers the existence of a HAV header in a packet can therefore conclude that a hash collision is possible if the HAV header is absent. Thus, it needs to simply remove the HAV header before retransmitting the packet, which may cause the packet to be dropped by recipients. Again, in doing so the malicious router causes the packet to be dropped not by itself, but by other routers in the network.

As shown in figure 7, $a$ is the source router and $X$ is the malicious router. At the source $a$, it generates a packet $p$, and stores the corresponding hash $h(p) = x$ in its DPD cache. The following packet $p'$ generated, has the same hash as the

previous packet, i.e. $h(p') = h(p) = x$. The source router $a$ is able to detect the hash collision by comparing it with the records in its DPD cache. Therefore, $a$ adds an HAV header as shown in figure 6, to avoid a possible collision by having a new hash value $h(p' + HAV) = x'$. When the malicious router $X$ receives packet $p'$, it can conclude that a collision might happen by removing the HAV header. On receiving packet $p$ at router $b$, a record with hash $h(p) = x$ is saved in the DPD cache. The consequence is that packet $p'$ cannot be distinguished by router $b$ after the HAV header being removed because it has the same hash $h(p') = x$.

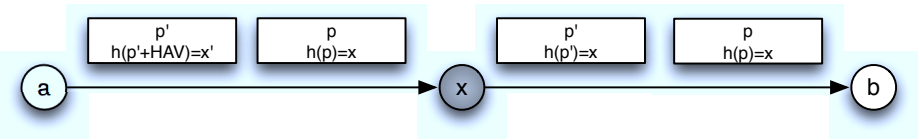


Figure 7: Attack based on the HAV field: The malicious router $X$ produces a hash collision by removing the HAV field.

Similarly, a malicious router can disrupt DPD by adding an HAV header option to a packet. This modified packet cannot produce the same hash value as the original packet, so it cannot be detected as a duplicate packet. This is similar to the attack in I-DPD, where a malicious router can change the sequence number for the same effect.

In figure 8, router $a$ forwards the packet $p$ with $h(p) = x$ to router $b$ and $x$. The malicious router $X$, instead of forwarding the original packet unmodified to $b$, adds an HAV header option with hash $h(p + HAV) = x' \neq x$. The router $b$ is unable to detect the duplicate packet and processes and forwards it as a new packet.

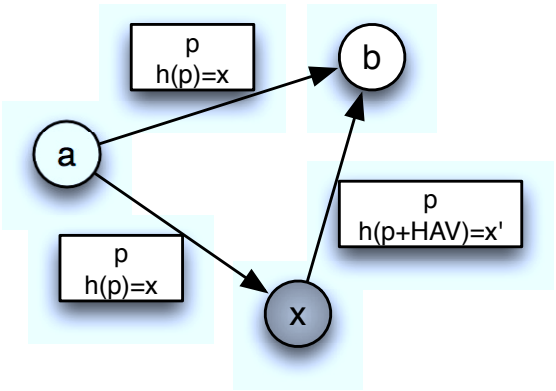


Figure 8: Attack by adding a HAV header option: The malicious router $X$ disables duplicate packet detection by adding a HAV header option.

Another possible attack for a malicious router is to transmit many packets with identical payload and IP header within a short time interval ("beacons"). This has several implications when H-DPD is used: (i) similar to a "jamming" attack, the increased load on the channel may lead to increased number of collisions of data and control traffic packets. (ii) An (adjacent) router receiving

such a beacon has to calculate and add a HAV header option to the packet header. This operation is time-consuming, and the packet has to be stored while the header option is generated. If a large number of beacons is received by a router, memory and CPU resources may thus be exhausted by this "Denial of Service" attack. (iii) When a packet is retransmitted by the adjacent router, an entry is stored in the hash cache for some amount of time. A large number of beacons within a short time may lead to an overflow of that buffer. Depending on what cache management is used, older – possibly "legitimate" – hash entries may be dropped from the cache, leading to an effective deactivation of the hash-based DPD mechanism.

# 3 Threat to Relay Set Selection Vector (RSSV)

Reduced Relay Set Selection (RSS) in SMF is achieved by distributed algorithms that dynamically calculate a topological Connected Dominating Set (CDS). Such algorithms are generally based on the presence of a neighbor discovery protocol, such as the "Neighborhood Discovery Protocol" (NHDP) [13], providing 1-hop and 2-hop neighborhood information. The relay set is then computed by using one from among a set of possible algorithms, such as E-CDS, S-MPR, etc. These algorithms are not interoperable, hence routers in a MANET must communicate to their neighborhood which algorithm(s) they respectively support. To this end, [1] defines a "Relay Set Selection Vector" (RSSV), by way of message and address block TLVs [14] to be used with the NHDP HELLO message exchange, allowing a router to declare which RSS algorithms it and its immediate neighbors support[2].

In SMF, two TLV types are defined for RSS algorithms:

- An SMF message TLV type, which is used to identify the existence of an SMF instance operating in conjunction with NHDP.
- An SMF address block TLV type, which is used to share the RSS algorithm configuration information among 2-hop neighbors.

In both TLVs, a value is assigned to represent each RSS algorithm.

## 3.1 RSSV Spoofing

Given the fact that there may be different RSS algorithms operating concurrently in the same network, a router will have to select relay sets according to compatibility of the algorithms operating in its immediate and 2-hop neighborhoods. A potential attack is, therefore, if a router – intentionally or otherwise – share false RSSV information for itself or for its neighbors.

For example, in figure 9, router *a* is about to select its relays. The following RSS algorithms are used in different routers:

- E-CDS: router *b, d, e*
- S-MPR: router *c, f, g*

[2]While several RSS are supported in the same *network*, it is not clearly specified in the current revision of SMF [1] whether a *router* can concurrently support several different RSS at the same time.

- MPR-CDS: router $h$

All routers, faithfully, declare their RSSV. Based on the messages from routers $b$, $h$ and $c$, router $a$ learns what algorithms are supported by both its direct neighbors and its 2-hop neighbors. This allows router $a$ to observe that while router $h$ provides topological coverage to all of the 2-hop routers ($d$, $e$, $f$, $g$), router $h$ runs an RSS algorithm different from all of $d$, $e$, $f$, $g$. Therefore, if $a$ selects $h$ as relay, $h$ may not be able to select relays among $d$, $e$, $f$, $g$ and thus packet forwarding beyond $d$, $e$, $f$, $g$ would not happen. Router $a$ also learns that router $b$ runs the same RSS algorithm as the 2-hop neighbors $d$, $e$, reachable via $b$ – and that router $c$ runs the same RSS algorithm as the 2-hop neighbors $f$, $g$, reachable via $c$. Router $a$ can therefore select $b$ and $c$ as relays, knowing that both of these will be able to not only provide coverage to all 2-hop neighbors, but also be able to select proper relays among these 2-hop neighbors.

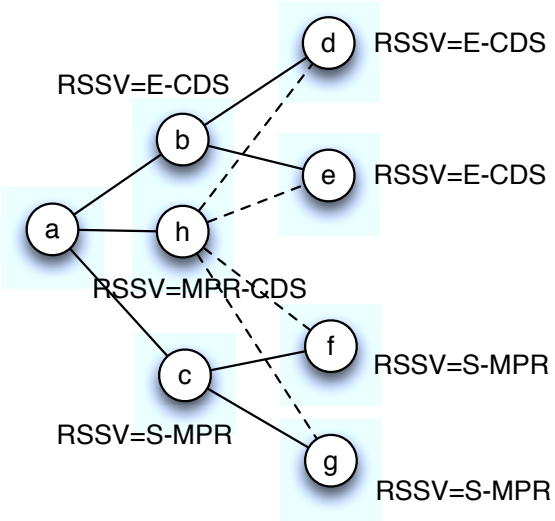


Figure 9: Relay set selection considering RSSV: Router $a$ makes the decision based on the RSSV declared by TLVs.

A malicious router, spoofing the RSSV of its 2-hop neighbors, is shown in figure 10: $X$ declares itself with *RSSV=MPR-CDS* in message TLVs, and further declares that $d$, $e$, $f$, $g$ have *RSSV=MPR-CDS*. Thus, router $a$ will choose $X$ as sole relay: from the information available to $a$, $X$ provides optimal topological coverage of the 2-hop neighborhood – and by running the same RSS as (declared for) all 2-hop neighbors, should be able to also do proper relay set selection with these. As a consequence, $X$ will "take control" of the multicast traffic in its neighborhood – in this case, be able to prohibit $b$ and $c$ from being selected as relays and, thus, if $X$ isnot actually forwarding traffic or performing RSS, disrupt network connectivity.

Finally, $X$ might simply declare that all other routers have (only) *RSSV=CF*, classical flooding, thus degrading the network performance to that of a simple flooding domain.

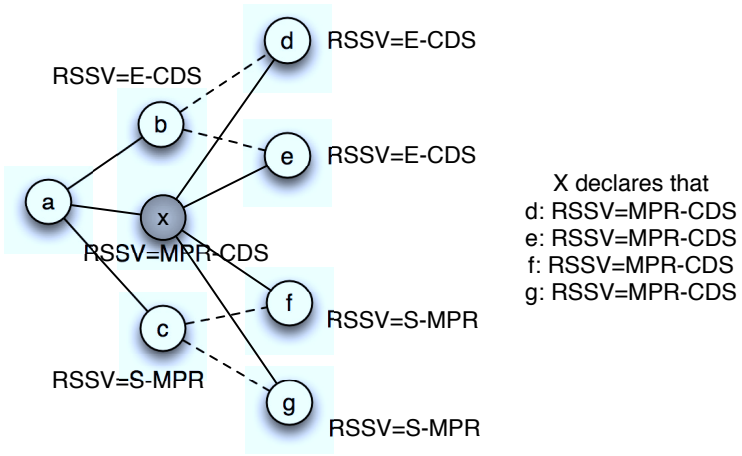


Figure 10: Attack on the RSSV to disrupt the relay set selection: The malicious router $X$ spoofs the RSSV of *d, e, f, g*.

### 3.2 RSSV Indirect Jamming

In a neighbor discovery based mechanism, a malicious router can intentionally and frequently alter the information declared – including the RSSV – so as to cause generation of inordinate amounts of control traffic by legitimate routers. Such *indirect jamming* is discussed in [15] for *neighborhood discovery* and *link state advertisement*, and also applies for the RSSV, which a malicious router may alter and signal frequently, causing its neighborhood to launch (possibly computationally intensive) RSS recalculations and signal selected relay set (causing increased channel occupation) as well as the change of its neighbor's status.

As shown in figure 11, the malicious router $X$ first declares itself as *RSSV=E-CDS* at $t_0$. Router $a$ will signal the change of its neighbor in its HELLO message at $t_1$ upon receiving the message from $X$. In a relatively short time, $X$ advertises in a HELLO that *RSSV=S-MPR*, and a link to another router $b$ at $t_1$. When $a$ receives this message at $t_2$, it will believe that $X$ has changed its status, then calculate its MPR set and broadcast a new HELLO message. The above action can be repeated to consume the power of $a$ and the bandwidth.

## 4 Threats to Relay Set Selection

[1] provides a framework for RSS, without requiring the use of any specific RSS algorithm. This section will, therefore, not explore the vulnerabilities of a specific RSS algorithm, but rather general threats to the framework of SMF relay set selection.

### 4.1 Eavesdropping

Eavesdropping is a common and easy passive attack in a wireless environment. Once a packet is transmitted, any suitable transceiver can potentially obtain a copy, for immediate or later decoding. Neither the source nor intended destination can detect this. As previously indicated, SMF uses a neighborhood

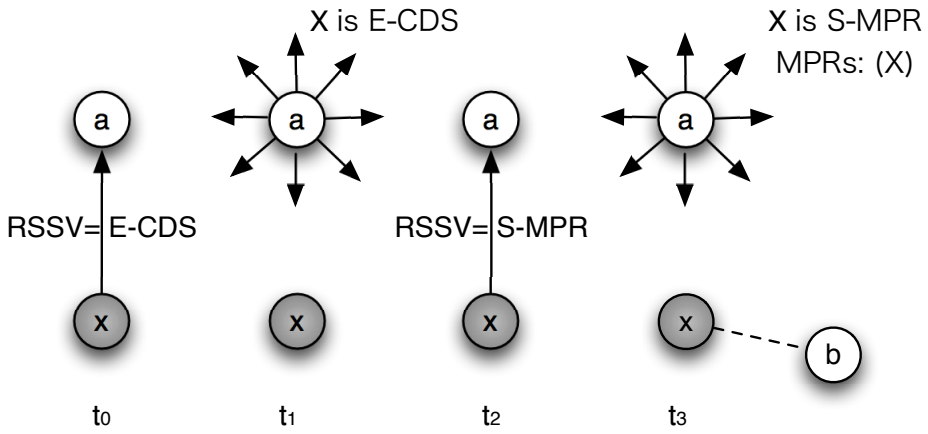


Figure 11: Indirect jamming in RSSV: The malicious router $X$ changes the declaration of its RSSV frequently to make router $a$ generate more control traffic.

discovery protocol for providing each router with 1-hop and 2-hop topological information. A malicious router can eavesdrop on the NHDP message exchange and thus learn this local topology information, as well as some source and destination addresses of data packets transmitted.

Eavesdropping will not have direct threat to the network nor to SMF, but it can provide crucial network information such as identity of communicating routers, link characteristic, router configuration, etc., enabling other attacks.

## 4.2 Message Timing Attack

As NHDP is used to make relay set selection decisions, vulnerabilities of this protocol also affect SMF operation. NHDP control messages define two types of timing information:

- Validity time, the time upon receipt during which the information contained within the message should be considered valid.
- Interval time, the time after which the next control message from the same router should be expected.

For *validity time*, since information contained in control messages is considered valid only for the duration indicated, an attacker can simply eavesdrop on NHDP messages from its neighbors, then instantly replay a received such message – but modified to have a low validity time, illustrated in figure 12. Router $b$ broadcasts a HELLO message with $valiTime = 6s$. Router $a$ receives the messages and marks the link between itself and $b$ is valid for 6 seconds. $X$ eavesdrops on the messages, obtains the identity of router $b$, then transmits the HELLO message with *valiTime=0.1s*. Receipt of this message by $a$ causes $a$ to replace previously received link information, and therefore consider the link between itself and $b$ as *invalid* after very short time (0.1 second). For SMF, this means that $b$ will not be selected as relay by $a$ even it may provide good connectivity to other parts of the network.

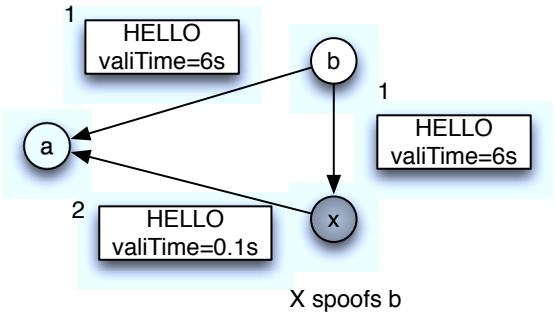


Figure 12: Validity timing attack: The malicious router $X$ spoofs $b$ and declares a short validity time of the link.

A similar threat is possible using the *interval time*, where a malicious router can behave as described above and also indicate a low interval time. The recipient of this message will expect a subsequent control message within this very short time – which will not arrive. As a consequence, the recipient decreases the link quality, or may even discard this link. Further vulnerabilities to the NHDP exist, described in [15].

## 4.3 Multicast Disruption

RSS algorithms are based on a router having topological information describing its 1-hop and 2-hop neighborhood. Thus, a malicious routers can spoof the links to or identities of other routers in the network, and thus disrupt connectivity and prevent multicast traffic from reaching parts of the network.

Figure 13 gives an example hereof, by way of link spoofing. The malicious router, $X$, eavesdrops on NHDP control traffic, and learns of the existence of $e$ and $f$ as 2-hop neighbors by way of $b$ and $c$, respectively. $X$ itself participates in NHDP, however declares (spoofs) in its control messages that it, too, has links to all neighbors of $b$ and $c$ – *i.e.,*declares the dotted links in figure 13. When $a$ is to select relays, it will choose $X$ as its relay – $X$ which may, then, simply not re-transmit any multicast traffic received and thereby disconnecting $e$ and $f$ from $a$.

A similar attack is possible by way of identity spoofing, as indicated in figure 14. The malicious router, $X$, eavesdrop on NHDP control traffic and learns of the existence of $c$ as a 2-hop neighbor by way of $b$. $X$ itself then commences participating in NHDP, but presenting itself under the same identity as $b$ – thus $a$ will see $c$ as a direct neighbor and not select $b$ as relay. As a consequence, $c$ is not able to receive multicast traffic, again being disconnected from the network.

## 4.4 Broadcast Storm

In MANETs, a broadcast storm caused by classical flooding is a serious problem because radio signals of two or more adjacent routers transmitting at the same time are likely to overlap. This can result in redundancy, contention and collisions [16]. Avoiding broadcast storms is one of the reasons why RSS algorithms are used – in SMF as well as in routing protocols such as [2].

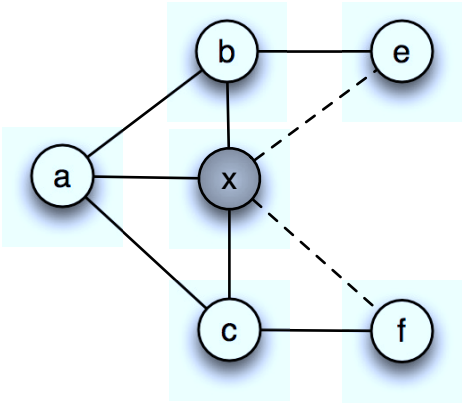


Figure 13: Multicast disruption by link spoofing: $X$ spoofs the link to $e$ and $f$.

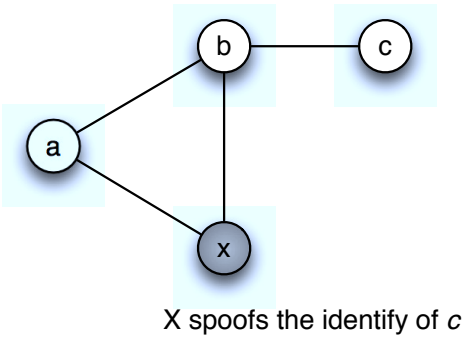


Figure 14: Multicast disruption by node spoofing. $X$ spoofs the identify of router $c$ to wipe $c$ from the multicast domain

In contrast to the attacks described in section 4.3, a malicious router may attack an SMF network by attempting to degrade RSS so as to produce classic flooding, illustrated in figure 15. Bold lines with arrows present the intended multicast traffic if the RSS algorithm run properly: *b, d, f, h* are selected as relays by *a*, and *c, e, g, i* just receive packets from *a* without forwarding.

A malicious router $X$ may disrupt this by overhearing NHDP control traffic, thus learning of the 1-hop neighborhood of *a*. $X$ may, then, generate control messages performing both identity spoofing and link-spoofing, pretending to be one of the 1-hop neighbors of *a* (*e.g.,* any or all of *b, c, d, e, f, g, h, i*) and declare that links to non-existing routers *e.g., z, x, y, v, w* exist for these, causing *a* to select more (or all) of its 1-hop neighbors as relays, degrading into classic flooding.

$X$ may overhear control messages from some of the 1-hop neighbors of *a* and thus learn of their 2-hop neighborhoods – and spoof links that it thus knows are non-existing. Such would be the case for *f* and *g*, for example. For *b* and *i*, $X$ may not know what their 2-hop neighbors are, however may "make an educated guess" when selecting links to spoof.

While this reduces network performance by disabling RSS and producing classical flooding, the effect of this attack is only local. Except if $X$ has accom-

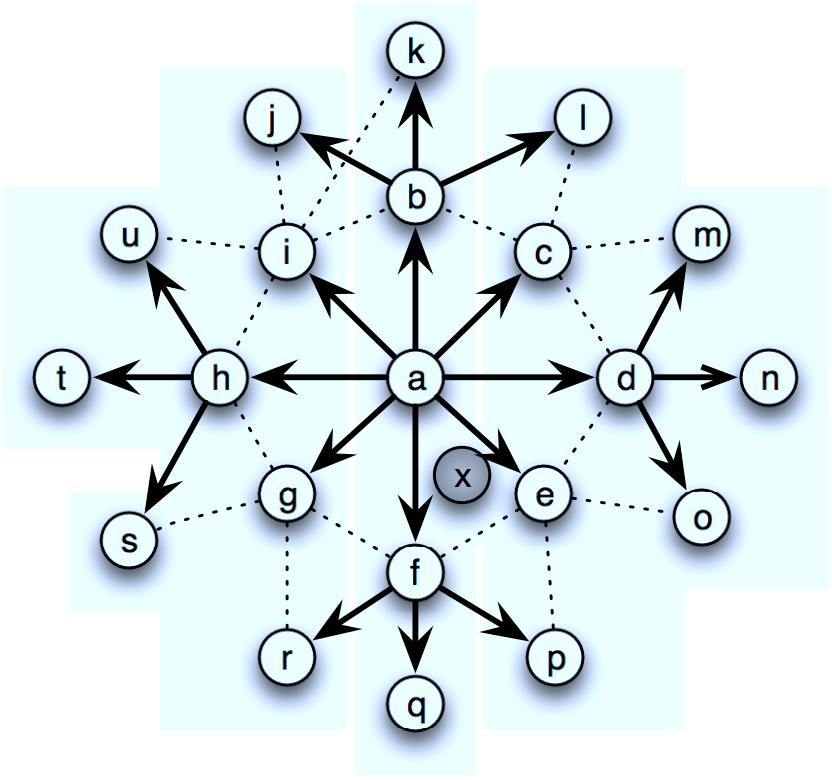


Figure 15: The broadcast storm attack: The bold line with arrow represents normal multicast traffic, and the dashed line the redundant traffic caused by having all the 1-hop neighbors of $a$ be selected as relays.

plices throughout the network, $b$, $c$, $d$, $e$, $f$, $g$, $h$ and $i$ likely will be able to select proper relay sets.

# 5 Conclusion

This memorandum has analyzed vulnerabilities of the "Simple Multicast Forwarding" (SMF) Protocol for Mobile Ad Hoc Networks. In addition to vulnerabilities inherited from its use of NHDP for acquiring local topology information allowing reduced relay set selection, SMF introduces two Duplicate Packet Detection mechanisms, each introducing additional vulnerabilities: disrupting network connectivity, as well as allowing a malicious router to incite other routers to produce unnecessary packet re-transmissions – thereby consuming precious channel resources.

SMF also provides a framework for enabling different relay set selection algorithms, to be used within SMF. As such algorithms may not be interoperable, this framework introduces a signaling mechanism (RSSV) whereby a router shares the algorithms it support itself – as well as the algorithms supported by its neighbors. Intended to allow a router to select its relays such that the RSS algorithms of these are compatible with algorithms of its 2-hop neighbors, the

RSSV also allows a malicious router to present conflicting or incorrect information, skewing relay set selection and possibly disrupting network connectivity.

Using NHDP for acquiring local topology, SMF inherits vulnerabilities of NHDP – and additionally also introduces vulnerabilities by way of eavesdropping, message timing attack, link spoofing, node spoofing, etc., allowing a malicious router to provoke connectivity disruption or a broadcast storm by degrading even RSS behavior to classical flooding.

# References

[1] J. Macker, "Simplified Multicast Forwarding," Internet Draft, draft-ietf-manet-smf-11, work in progress, March 2011.

[2] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," Experimental RFC 3626, October 2003.

[3] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying: An efficient technique for flooding in mobile wireless networks," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, January 2001.

[4] T. Clausen, P. Jacquet, E. Baccelli, and D. Nguyen, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks," Experimental RFC 5449, February 2009.

[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Experimental RFC 3561, July 2003.

[6] T. Clausen, L. Viennot, and P. Jacquet, "Optimizing Route Length in Reactive Protocols for Ad Hoc Networks," in *Proceedings of the IFIP MedHocNet*, September 2002.

[7] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," Standards Track RFC 3686, 2004.

[8] R. Ogier and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding," Experimental RFC 5614, 2009.

[9] T. Clausen, C. Dearlove, and P. Jacquet, "The Optimized Link State Routing Protocol version 2," Internet Draft, draft-ietf-manet-olsrv2-11, work in progress, April 2010.

[10] P. Jacquet and E. Baccelli, "Diffusion mechanisms for multimedia broadcasting in mobile ad hoc networks," in *Proceedings of the IASTED International Conference on Internet and Multimedia Systems and Applications (IMSA)*, August 2004.

[11] T. Clausen, L. Viennot, T. Olesen, and N. Larsen, "Investigating data broadcast performance in mobile ad-hoc networks," in *Proceedings of the International Symposium on Wireless Personal Multimedia Communications (WPMC)*, October 2002.

[12] S. Kent and R. Atkinson, "IP Authentication Header," Standards Track RFC 2402, November 1998.

[13] T. Clausen, C. Dearlove, and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)," Standards Track RFC 6130, April 2010.

[14] T. Clausen, C. Dearlove, J. Dean, and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format," Standards Track RFC 5444, February 2009.

[15] U. Herberg and T. Clausen, "Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRV2)," *International Journal of Network Security & Its Applications*, vol. 2, no. 2, pp. 162–181, 2010.

[16] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wireless Networks*, vol. 8, pp. 153–167, March 2002.

# Contents

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 Orsay Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399